Applicant respectfully does not understand this objection. This specification does not use parenthesis to indicate flow chart decisional steps, and no such implication was ever intended. Rather, parenthesis are used in the specification when they are appropriate pursuant to normal English grammar.

For example, if a sentence is introduced with a phrase such as, "In step 1000, . . . ", no parenthesis are used around the words "step 1000". If parenthesis were used, then the sentence introduction would read, "In (step 1000), ...", which is not grammatically proper usage of parenthesis.

Parenthesis are used in the specification in order to mention a flow chart reference without affecting the flow of a sentence. For example, the specification is sometimes worded as follows: "After x, y, z happens (step 1000), then a, b, c happens (step 1002)." The reader can remove the two parenthetical designations from the sentence, and the resulting sentence would still make perfect sense ("After x, y, z happens, then a, b, c happens."). Applicant's specification therefore uses parenthesis where appropriate for readability and grammatical correctness. There is no implication that parenthetical designations represent decisional steps whereas non-parenthetical references represent non-decisional steps.

Having said that, if the Examiner is aware of some rule, MPEP Section, or other document, which establishes a rule that parenthetical flow chart designations represent decisional steps whereas non-parenthetical flow chart references represent non-

decisional steps, applicant respectfully requests that the Examiner bring this document to the attention of the undersigned. Applicant will then be pleased to make the necessary changes in the specification.

In paragraph 4.b. of the Office Action, the Examiner indicated that at page 28, line 2, the designation "(step 512)." should be inserted after "I.D.". This has been done.

In paragraph 4.c. of the Office Action, the Examiner indicated that at page 35, line 5, "in" should be replaced after "104" and "()" be removed from "(step 1016)." because step 1016 is not one of decision. Again, however, Applicant objects to any change in his chosen wording for the specification solely due to an incorrect assumption on the part of the Examiner that parenthesis around a flow chart designation must imply that the referenced flow chart step is one of decision.

In fact, the change requested by the Examiner in this paragraph 4.c. points out exactly the reason why Applicant used parenthesis in this instance. In particular, if the changes requested by the Examiner in paragraph 4.c. were made, then the sentence would read, ". . . and transmits the result back to the certification server 104 in step 1016." Such a sentence would then be incorrect, since the certification server 104 is <u>not in</u> step 1016.

Applicant's use of parenthesis in this sentence improves readability and makes the sentence say what is meant. Again, however, should the Examiner bring to Applicant's attention a

document establishing a rule that parenthetical flow chart descriptions must represent decisional steps, Applicant will find a way to reword this sentence such that it satisfies the rule and still says what is meant. For now, however, Applicant respectfully declines to make the requested change.

II. REJECTIONS UNDER 35 U.S.C. § 102

The Examiner rejected claims 1-6, 18-21, and 29-31 under 35 U.S.C. § 102(e) as being anticipated by *Ensor*.

Ensor teaches a user-transparent security method and apparatus for authenticating user terminal access to a network. However, it is only the equipment which is authenticated, not the user him or herself. This can be seen from the summary of the invention, at *Ensor's* column 2, lines 32-52 (also cited by the Examiner).

As can be seen, when access is first made to the network, the network control center automatically detects, selects and encrypts the "network coupling identifier" to derive a password for the newly arrived user terminal. The network control center stores this password into the memory of the user terminal. Later, upon subsequent connection to the network by the same user terminal, the control center again generates another encrypted password using a newly detected network coupling identifier, and compares it to the password which had been previously stored on the user terminal.

The "network coupling identifier", which is used to generate the password is an attribute of the user terminal and not the user him or herself (see, for example, *Ensor* column 2, lines 23-30, in

which she mentions one embodiment in which the network coupling identifier is a telephone number, and another embodiment in which the network coupling identifier is the network address of a particular terminal, server or user directory.) Nothing in *Ensor's* process takes into account the identity of the user of the terminal at any time. The only thing that is authenticated is the terminal itself, not the person or persons using the terminal.

In fact, *Ensor* makes a point of performing the authentication process without the user him or herself even knowing that such authentication is taking place (for example, see *Ensor* column 2, lines 37-38, "the password is then downloaded into memory of the user terminal unbeknownst to the user.")

All of Applicant's rejected claims, on the other hand, call for the creation of a signature which depends upon both a user identity and the user system. As described in Applicant's specification, the user identity can be specified by such means as a PIN number or code, for example. Other examples include a user pass-phrase, a user biometric, or any other attribute that the user either has or knows. It is the combination of these two elements - one identifying the user and one identifying the system being used - which is called for in Applicant's rejected claims.

The difference between Applicant's claimed method and that taught by *Ensor* is important, because without including a user identity in the signature, *Ensor's* network control center has authenticated only the machine (user terminal) that has connected to her network. It has not authenticated the user him or herself.

For example, *Ensor's* technique does not necessarily prevent unauthorized access to the network by an imposter who has stolen the rightful user's terminal equipment, or who has otherwise gained unauthorized physical access to the rightful user's terminal equipment. *Ensor's* technique contains no protection against this kind of subversion. But by calling for the signature to depend upon both a user identity and the user system in combination, the techniques of Applicant's rejected claims provided a heightened level of confidence that the user accessing a network is, in fact, the same user who accessed the network originally.

In the first full paragraph of page 5 of the Office Action, the Examiner argues that the use of user identities is "deemed inherent" to *Ensor* because the telephone number of the user terminal constitutes *Ensor's* user identity. Applicant respectfully disagrees. Applicant's rejected claims call for the creation of a signature in dependance upon two items: a user identity and a user system. The Examiner's position, however, requires that the telephone number which identifies the user system also identifies the user. If such were the case, then *Ensor's* signature would be based on only one item, namely the telephone number of the user terminal. That is not what is called for in Applicant's rejected claims.

Applicant's specification makes clear that it is the combination of the two different components which provides the added security achieved by the invention as called for in these claims. As pointed out in Applicant's specification at page 9,

lines 17-24, among other places, the methods of these claims minimize the risk of a stolen PIN, because the PIN is useless without the computer system hardware on which the first user identity was originally established, and also minimize the risk of subversion through the theft of the first user's computer hardware, because a transaction will not be authorized without the user's PIN. *Ensor's* technique does not provide both protections.

Applicant will now review each of the rejected claims and point out specific language which distinguishes over *Ensor*.

A. Independent Claim 1.

Claim 1 call for, among other things, a step of storing a first signature "dependent upon a first user identity and a first system in combination."

Ensor does not use any first "user identity" to generate her passwords. Instead, *Ensor's* technique uses only a "network coupling" identifier, which identifies hardware, not an individual user.

Nor can the term "user identity" as used in Applicant's claim, be stretched to include an item (such as *Ensor's* network coupling identifier) which depends only on hardware. Applicant's specification makes clear that the term "user identity" must depend on the user him or herself, not the hardware with which he or she accesses the network.

Accordingly, it is respectfully submitted that claim 1 should be patentable.

B. Independent Claim 18.

Claim 18 calls for, among other things, a step of forming a first signature "dependent upon a first user identity and a first user system in combination." Again, for the reasons set forth above with respect to claim 1, this claim should be patentable over *Ensor*.

C. Independent claim 29.

Claim 29 calls for, among other things, a step of storing a first signature "dependent upon a first user identity and a first user system in combination." Again, as with claim 18, this claim should be patentable for at least the same reasons as set forth above with respect to claim 1.

D. Dependent Claims 2-6, 19-21, and 30-31.

These claims all depend ultimately from independent claim 1, 18 or 29, all of which should now be patentable. These dependent claims should therefore be patentable for at least the same reasons as their respective independent parent claims. In addition, it is submitted that these claims all add their own limitations which render them patentable in their own right.

III. REJECTIONS UNDER 35 U.S.C. § 103(a)

The Examiner rejected claims 7-9 under 35 U.S.C. § 103 over a combination of *Ensor* and *Davis*.

Claims 7-9 all depend ultimately from independent claim 1, and should therefore be patentable for at least the same reasons. Applicant respectfully submits that these claims also add their own

limitations which should render them patentable in their own right as well.

IV. ALLOWABLE AND ALLOWED CLAIMS

The Examiner objected to claims 10-15, 22-25 and 32-38 solely as being dependent upon a rejected base claim. Since the base claims are now believed to be patentable, it is respectfully submitted that these claims should now be patentable as well.

Claims 16-17 and 26-28 have been allowed.

V. CONCLUSION

In light of the above, it is respectfully submitted that all of the claims now pending in the application should be allowable, and reconsideration of the rejections is requested.

Respectfully submitted,

Date: 8/16/99

By: Warren S. Wolfeld
Warren S. Wolfeld
Reg. No. 31,454

FLIESLER, DUBB, MEYER & LOVEJOY LLP
Four Embarcadero Center, Suite 400
San Francisco, California 94111-4156
Telephone: (415) 362-3800